L'utilisation des nouvelles technologies par le secteur financier face au droit à la vie privée et à la protection des données

De Terwangne, Cécile

Published in:
The increasing impact of human rights law on the financial world

Publication date:
2016

Document Version
le PDF de l'éditeur

L'utilisation des nouvelles technologies par le secteur financier face au droit à la vie privée et à la protection des données

Cécile DE TERWANGNE

Professeur à la faculté de droit de l'Université de Namur
Directrice de recherche au CRIDS
(Centre de Recherche Information, Droit et Société)

I. Introduction

La relation que les institutions financières nouent avec leurs clients se nourrit d'une quantité impressionnante d'informations, qu'il s'agisse des données recueillies lors de l'amorce de cette relation ou de celles découlant de l'utilisation des services bancaires et financiers. Le recours massif aux paiements électroniques sous toutes leurs formes (via la carte de banque, la carte de crédit, les paiements *online*) draine vers les institutions financières des myriades de traces des opérations effectuées par les clients, indiquant au passage les lieux fréquentés, les achats effectués, les loisirs, les moyens de locomotion et la localisation. Dans nombre de cas, le client fournit lui-même des informations le concernant, mais bien souvent également ce sont des tiers qui les transmettent ou les banques qui se les procurent à d'autres sources. Les institutions financières sont donc « assises sur une montagne d'informations… montagne d'or qui fait rêver les géants de l'Internet »[1]. Ces informations, pour la plupart, relèvent de la catégorie des « données à caractère personnel » et sont dès lors couvertes par la législation relative à la protection de telles données. Il n'est donc pas question d'imaginer un libre usage de cette manne à grande valeur économique et sociale à l'heure du *Big data*.

En Belgique, à ce jour, c'est la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (dite « loi vie privée ») qui assure cette protection. Cette loi, dans sa version modifiée le 11 décembre 1998, a transposé la directive européenne 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre cir-

[1] M. LEBLANC-WOHRER, « Le défi de la protection des données personnelles », *L'AGEFI Hebdo*, 5 juin 2014, www.agefi.fr/banque-assurance/actualites/hebdo/20160210/defi-protection-donnees-personnelles-154345.

culation de ces données[2]. Or, il s'est peu à peu avéré nécessaire de revoir la directive pour la mettre en phase avec les développements techniques et sociétaux qui se sont fait jour depuis son adoption en 1995, à une époque où Internet n'en était qu'à ses balbutiements. Ce travail de révision vient d'arriver à son terme et a pris la forme d'un règlement européen[3], norme destinée à unifier et non plus seulement harmoniser les règles applicables à travers l'Europe.

Les pages qui suivent présentent les règles de protection des données applicables aux institutions offrant des services financiers, en tenant compte de ce règlement général sur la protection des données (ci-après « RGPD ») qui va prendre le relais de la loi de 1992, même si celui-ci ne sera d'application que deux ans après son entrée en vigueur, soit en mai 2018.

Avant d'entrer dans le détail de l'analyse, il est impératif pour ceux qui ont à appliquer la loi vie privée dans le secteur financier, de prendre conscience de la nouvelle dimension que la notion de « vie privée » a acquise. La vie privée, dans ce contexte, ne doit pas se comprendre comme limitée à un ensemble d'informations personnelles ou d'images que l'on souhaite garder cachées, ou à des actions que l'on mène derrière un mur, à l'abri des regards et des interférences. Elle est à entendre comme autodétermination, comme autonomie et, plus particulièrement, comme autonomie informationnelle, c'est-à-dire l'autonomie dans la détermination des conditions d'usage et de communication des informations qui se rapportent à soi-même. La vie privée, c'est, en ce sens, la maîtrise par chacun de son image informationnelle[4].

II. Notions principales et champ d'application

A. Donnée à caractère personnel

La notion de « donnée à caractère personnel » est particulièrement large. Elle englobe toute information qui concerne une personne physique identifiée ou identifiable (appelée la « personne concernée »)[5].

Il s'agit donc d'un concept plus large que celui d'information privée ou d'information confidentielle. La notion couvre des informations de toute nature (confidentielles, privées, professionnelles, publiques) et de toute forme (écrits, photos, sons, données de localisation, données de comportement en ligne, données biométriques, etc.). Le numéro de carte bancaire, les opérations effectuées sur un compte, les informations

[2] La loi du 11 décembre 1998 transpose la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

[3] Règlement 2016/679 du Parlement et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, 4 mai 2016.

[4] C. DE TERWANGNE, « The Right to be Forgotten and the Informational Autonomy in the Digital Environment », *The Ethics of Memory in a Digital Age: Interrogating the Right to Be Forgotten*, Palgrave, octobre 2014, pp. 85 et 86.

[5] Article 1er, § 1er, de la loi du 8 décembre 1992.

liées à l'usage d'une carte de crédit sont autant de données à caractère personnel. « En ce qui concerne les services bancaires par téléphone, où la voix du client qui donne des instructions à la banque est enregistrée, il y a lieu de considérer ces instructions enregistrées comme des données à caractère personnel. »[6]

Il peut par ailleurs s'agir d'informations « objectives » telles que les coordonnées privées ou professionnelles d'un individu, ou d'informations « subjectives », présentées sous forme d'avis, d'évaluations ou d'appréciations. « Ce dernier type de renseignements représente une grande partie du traitement des données à caractère personnel dans des secteurs tels que celui des banques, pour l'évaluation de la fiabilité des emprunteurs ("X est un emprunteur fiable"). »[7]

La seule limite de la notion de donnée à caractère personnel est que la donnée doit se rapporter à une personne physique. La notion ne couvre donc pas les données concernant les personnes morales telles les sociétés, les ASBL, les communes… Elle ne couvre pas non plus les données se rapportant aux personnes décédées[8].

L'élément important pour cerner la notion de donnée à caractère personnel est que la personne à laquelle se rapporte l'information soit identifiée ou identifiable, c'est-à-dire que cette personne puisse être identifiée « directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[9]. Le règlement européen précise clairement que la protection des données vaut aussi pour les cas où l'identification est réalisable via un identifiant en ligne (une adresse IP) ou via des données de localisation[10]. L'identification dont il est question doit se comprendre non comme l'établissement de l'identité civile d'un individu, mais comme *l'individualisation* de cette personne, la capacité de la traiter différemment des autres[11].

Seules les données anonymes sont hors du champ d'application de la protection des données. Une donnée sera considérée comme anonyme lorsqu'elle ne peut pas ou

[6] Groupe de l'article 29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP 136*, 20 juin 2007, p. 9, http://ec.europa.eu/justice/policies/privacy.

[7] *Ibid.*, p. 7.

[8] Commission de la protection de la vie privée, *Rapport annuel 2011*, point 7.7. Également : *Vade-mecum relatif à la recherche biomédicale*, 2011, p. 6, disponible à l'adresse www.privacycommission.be/sites/privacycommission/files/documents/vade-mecum-recherche-biomedicale_0.pdf. Voy. aussi considérant 27 du RGPD.

[9] Article 1er, § 1er, de la loi du 8 décembre 1992.

[10] Article 4, 1°, RGPD.

[11] Voy. le considérant 36 du RGPD, qui reprend le contenu du considérant 36 de la directive 95/46 avec l'ajout mis en évidence ci-après : « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, *tels que le ciblage.* » Le terme « ciblage » correspond, dans la version anglaise qui a été la version de travail du législateur européen, à « singling out » qui peut aussi se traduire par « individualisation ».

plus être mise en relation avec une personne identifiée ou identifiable[12]. Les données codées c'est-à-dire les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code[13] sont, quant à elles, bien couvertes, car le lien n'est plus évident mais n'est pas rompu entre l'information et la personne concernée. Ces données pseudonymes doivent donc être considérées comme des données à caractère personnel.

Quant aux données anonymes, il est important de réaliser que l'anonymat d'aujourd'hui n'est pas d'office celui de demain et que cet anonymat doit être reconsidéré régulièrement au vu des développements techniques et des possibilités de croisement des données, notamment dans le cadre du *Big data*, qui pourraient amener à un certain moment à réévaluer le caractère anonyme des données et à les faire rentrer dans la catégorie des données à caractère personnel et dès lors dans le champ de la loi.

B. Traitement de données

On entend par «traitement de données» toute opération ou tout ensemble d'opérations appliquées à des données personnelles[14]. Les opérations dont il s'agit sont particulièrement variées et comprennent la collecte de données, leur conservation, l'utilisation, la modification, la communication, etc. En fait, tout ce qui peut être fait avec des données à caractère personnel, tout type d'actions ou d'utilisations des données entre dans la définition de «traitement».

C'est la finalité attachée à un ensemble d'opérations appliquées à des données à caractère personnel qui donnera à ces différentes opérations leur cohérence et permettra de conclure que l'ensemble forme un traitement de données. La finalité est l'élément unificateur du traitement[15]. La finalité de gestion du personnel, par exemple, implique une grande variété d'applications qui peuvent être envisagées comme formant un tout, un seul traitement visant à la gestion du personnel.

Un traitement peut poursuivre plusieurs finalités, mais celles-ci doivent être compatibles entre elles pour être jugées comme attachées au même traitement. Si une finalité n'est pas compatible avec la première[16], elle se rattache alors à un traitement différent du premier.

[12] Article 1, 5°, de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

[13] Article 1, 3°, de l'arrêté royal du 13 février 2001.

[14] Article 1er, § 2, de la loi du 8 décembre 1992.

[15] Th. LÉONARD et Y. POULLET, «La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995», *J.T.*, 1999, p. 379; Th. LÉONARD, «La protection des données à caractère personnel et l'entreprise», *Guide juridique de l'entreprise*, 2e éd., titre XI, liv. 112, Diegem, Kluwer, 1996, p. 15.

[16] Voy. *infra* ce qu'est une finalité compatible.

C. Champ d'application matériel

La loi vie privée s'applique dès que les opérations effectuées sur des données personnelles se réalisent, ne fût-ce qu'en partie, par des moyens automatisés. Les moyens automatisés englobent toutes les technologies de l'information: informatique, télématique, réseaux de télécommunications (Internet), puces, géolocalisation... La loi s'applique donc, par exemple, à la liste électronique des opérations effectuées sur un compte en banque ou au fichier informatisé du personnel d'une entreprise.

Quand les opérations sur les données se font sans le moindre recours à des procédés automatisés (sur papier ou microfiches, notamment), il faut tout de même respecter la loi si les données figurent ou sont destinées à figurer dans un fichier manuel, c'est-à-dire un ensemble dans lequel les données sont accessibles selon des critères spécifiques (par exemple, un classement sur la base des noms des personnes, par ordre alphabétique).

D. Champ d'application territorial

Ni la nationalité des personnes concernées, ni leur lieu de résidence habituelle, ni la localisation physique des données à caractère personnel ne sont déterminants pour décider de l'application de la loi belge à une situation de traitement de données.

Les critères à prendre en considération pour déterminer si la loi belge est applicable sont le lieu d'établissement du responsable du traitement[17] (critère principal) et, dans le cas où ce responsable se trouverait en dehors de l'Union européenne, la localisation des moyens utilisés (critère secondaire).

1. Détermination du responsable du traitement

Il convient de déterminer tout d'abord qui est le responsable du traitement.

La loi ne donne pas une réponse systématique à la question de la désignation du responsable. En revanche, elle fournit les critères permettant d'identifier ce dernier. D'après l'article 4, § 1er, de la loi, le responsable du traitement est la personne qui, seule ou conjointement avec d'autres, détermine les objectifs et les moyens de ce traitement de données. Il peut s'agir d'une personne physique ou morale ou même d'une association de fait.

Étant donné que la qualité de responsable du traitement dépend des deux critères énoncés ci-dessus, la désignation concrète des responsables de traitement est affaire de cas par cas. Dans le cas d'une institution financière, le responsable de certains des traitements effectués au sein de l'institution sera l'institution elle-même, en tant que personne morale, tandis que pour d'autres traitements, cela pourra être un de ses départements ou un service, selon le niveau de prise de décision relativement aux traitements de données mis en place.

[17] Article 3*bis*, alinéa 1er, 1°, de la loi du 8 décembre 1992.

2. *Critère de l'établissement fixe du responsable du traitement*

La loi vie privée s'applique lorsque les données sont traitées dans le cadre des activités d'un établissement fixe[18] du responsable du traitement localisé sur le territoire belge[19]. L'établissement sur le sol belge suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable.

Une institution financière faisant partie d'une structure «internationale» présente dans plusieurs États devra tout de même respecter la loi belge pour les activités déployées dans l'entité établie sur le territoire belge. La dépendance de cette institution à l'égard d'une entité mère ou son intégration complète dans une société de droit étranger est sans incidence sur la règle d'application de la loi belge de protection des données. La situation des institutions faisant partie d'une multinationale ou, à tout le moins, présentes dans plusieurs États membres de l'Union européenne sera toutefois simplifiée dès la mise en application du RGPD, étant donné que celui-ci a vocation à s'appliquer uniformément sur l'ensemble du territoire européen. Les mêmes règles seront donc applicables à l'ensemble des acteurs, quel que soit l'État où ils sont établis. Seuls les points de droit pour lesquels une marge de manœuvre est encore réservée aux États membres auront une application limitée à la juridiction de chaque État.

3. *Critère de la localisation des moyens utilisés*

À l'instar du législateur européen[20], le législateur belge a manifesté son souci que les traitements de données présentant un lien étroit avec notre territoire, mais effectués par un responsable se situant en dehors des frontières, ne se retrouvent pas dépourvus de protection. Afin d'éviter pareille situation, l'article 3*bis* de la loi du 8 décembre 1992[21] prévoit que tout responsable qui n'est pas établi de manière permanente sur le territoire de l'Union européenne, mais qui recourt à des moyens, automatisés ou non, situés sur le territoire belge, dans le but de traiter des données personnelles, est soumis à cette loi. Il est tenu, en outre, de désigner un représentant établi sur le territoire belge[22]. Le seul transit de données sur le territoire belge n'est toutefois pas couvert par la loi.

L'exposé des motifs de la loi du 11 décembre 1998 signale que «le terme "moyens" recouvre tout équipement possible, tels les ordinateurs, les appareils de télécommunications, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routes, etc.»[23].

Ce critère secondaire a suscité bien des difficultés d'application dans le contexte d'Internet et d'un monde en réseau. Il sera abandonné lors de la mise en application du règlement européen. Ce texte prévoit de retenir deux nouveaux critères en lieu et place de la localisation des moyens utilisés pour traiter les données, dans le cas où le responsable du traitement n'est pas établi sur le sol européen. Ainsi, aux termes de l'article 3, § 2, du RGPD, «Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.»

C'est donc le fait qu'un traitement de données soit lié à une offre de biens ou de services qui vise des personnes se situant sur le territoire européen ou au suivi du comportement de ces personnes (de leur activité sur le Web, grâce à des *cookies*, par exemple) qui sera déterminant pour conduire à l'application du règlement européen à ce traitement.

III. Les principes fondamentaux de la loi

Pour être admissibles aux yeux de la loi, les traitements de données opérés doivent répondre à plusieurs conditions. Ces conditions tiennent, d'une part, aux traitements eux-mêmes et, d'autre part, aux données traitées. Ainsi donc, pour être licite, un traitement de données à caractère personnel doit être loyal et transparent (principe de loyauté), doit poursuivre une finalité déterminée, explicite et légitime (principe de finalité) et s'identifier à une des hypothèses reprises dans la liste de l'article 5 de la loi de 1992 (principe de proportionnalité). En outre, seules les données respectant les principes de finalité et de proportionnalité peuvent faire l'objet du traitement. Les données doivent, enfin, présenter des qualités d'exactitude et de mise à jour.

Le non-respect de chacune des conditions mentionnées ci-dessus et présentées dans les pages qui suivent est punissable pénalement: d'une amende et/ou d'un emprisonnement en cas de récidive.

[18] Le considérant 19 de la directive 95/46/CE précise que «l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. [...] La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à ce sujet».

[19] ... ou en un lieu où la loi belge s'applique en vertu du droit international public (article 3*bis* de la loi).

[20] Voy. considérant 20 de la directive 95/46: «considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés».

[21] Article 3*bis*, alinéa 1er, 2°, de la loi du 8 décembre 1992.

[22] Article 3*bis*, alinéa 2, de la loi du 8 décembre 1992.

[23] Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 27.

A. Le principe de loyauté

Aux termes de l'article 4, § 1er, 1°, de la loi vie privée, les données à caractère personnel doivent être traitées loyalement et licitement. L'exigence de loyauté induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données.

Le principe de loyauté est donc lié au devoir de transparence qui sera exposé dans des développements ultérieurs. Ce devoir de transparence implique que certaines informations soient fournies spontanément par le responsable du traitement aux personnes concernées. L'obligation de fournir des informations est à géométrie variable, liée précisément à l'exigence de loyauté: au-delà de certains renseignements à donner en toutes circonstances, d'autres informations ne sont à transmettre que si cela est nécessaire pour garantir la loyauté du traitement des données. Ces informations supplémentaires portent sur les destinataires des données traitées, le fait que les données seront transmises au-delà des frontières, etc. L'idée, on le voit, est d'annoncer loyalement aux personnes concernées le sort qui attend leurs données.

La loyauté du traitement de données ne se limite pas à la collecte, mais doit être garantie à toutes les étapes de celui-ci.

Dans certaines circonstances, le devoir de loyauté implique que préférence soit donnée à la collecte de données directement auprès des personnes concernées, et non pas de manière indirecte auprès de sources tierces[24]. C'est le cas dans un contexte d'emploi, notamment lors des procédures de recrutement des employés[25]. En présence de données médicales, également, le principe édicté par la recommandation n° R(97)5 du Comité des ministres du Conseil de l'Europe relative aux données médicales[26] consiste en ce que «les données médicales doivent en principe être collectées *auprès de la personne concernée*. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 4, 6 et 7 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données»[27].

B. Le principe de finalité

Principe clé de la protection, le principe de finalité exige que tout traitement poursuive une ou des finalité(s) déterminée(s), explicite(s) et légitime(s) (point 1 ci-après), que l'on ne fasse que ce qui est compatible avec cette (ces) finalité(s) (point 2), que l'on ne traite que les données pertinentes au vu de la (des) finalité(s) (point 3) et que l'on

[24] V. VERBRUGGEN, *Les Codes commentés. La protection des données*, Bruxelles, Larcier, 2011, pp. 55 et 56.

[25] Recommandation n° CM/Rec(2015)5 du 1er avril 2015 du Comité des ministres du Conseil de l'Europe sur le traitement des données à caractère personnel dans le cadre de l'emploi, point 5.1.

[26] Au point IV, B. «Le droit d'accès».

[27] V. VERBRUGGEN, *Les Codes commentés. La protection des données, op. cit.*, p. 55.

ne conserve ces données qu'aussi longtemps que cela est nécessaire pour atteindre la finalité du traitement (point 2).

1. Finalité du traitement déterminée, explicite et légitime

L'article 4, § 1er, 2°, de la loi vie privée prescrit que les données à caractère personnel «doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables».

a. Finalité déterminée

Tout traitement de données doit poursuivre une ou des finalité(s) déterminée(s). Il s'agit de savoir, dès le démarrage d'un traitement de données, quel(s) objectif(s) ce traitement est appelé à servir. La finalité ne peut être inexistante («on ne sait pas encore à quoi vont servir ces données, mais comme on a l'occasion de les collecter, collectons-les toujours») ni floue.

La spécification de la finalité est fondamentale, car c'est elle qui va déterminer le traitement de données à caractère personnel et permettre à la personne concernée de contrôler le sort réservé aux données la concernant[28].

La finalité doit être précise afin de permettre à la personne concernée d'effectuer cette analyse et d'exercer les droits qui lui sont conférés par la loi. Cette précision permettra également au responsable du traitement de déterminer les données qui devront être collectées et traitées. En effet, comme on le verra plus loin, les données traitées doivent être pertinentes au regard de la finalité. Une finalité qui ne serait pas suffisamment précise et serait donc énoncée de manière trop large permettrait de traiter un ensemble bien trop vaste de données, toutes pouvant passer pour pertinentes par rapport à la finalité annoncée.

On peut trouver, dans la liste des finalités proposée sur son site par la Commission de la protection de la vie privée afin d'aider les responsables de traitement à effectuer la formalité de déclaration[29], des modèles de finalités déterminées avec suffisamment de précision. On trouve, par exemple, dans cette liste «administration du personnel», «contrôle sur le lieu de travail», «lutte contre la fraude et les infractions de la clientèle», «collecte de dons», «relations publiques», «gestion du contentieux», «octroi de crédit», «service de courtage», etc.

[28] M.-H. BOULANGER, C. DE TERWANGNE et Th. LÉONARD, «La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel», *J.T.*, 1993, p. 377; M. VAN OVERSTRAETEN et S. DEPRÉ, «Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique», *Rev. trim. dr. h.*, 2003, pp. 685 et 686.

[29] Cette formalité de déclaration de tout traitement automatisé de données va disparaitre lors de la mise en application du règlement européen

Déterminer la finalité poursuivie par le traitement de données à caractère personnel se révèle donc une étape essentielle en matière de protection des données à caractère personnel.

b. Finalité explicite

La finalité doit également être explicite, ce qui signifie qu'elle doit être annoncée, ne pas être tenue « secrète » ou « camouflée »[30].

La transparence des traitements de données fait partie intégrante du régime de protection. La ou les finalités du traitement entrepris sont parmi les éléments les plus importants à communiquer au nom de l'obligation de transparence. L'information sur la finalité poursuivie doit être systématiquement dévoilée lors de la mise en œuvre de tout traitement.

c. Finalité légitime

Enfin, la finalité doit être légitime, ce qui signifie que la finalité ne peut induire une atteinte disproportionnée aux droits, libertés et intérêts en jeu, au nom des intérêts poursuivis par le responsable du traitement[31]. La notion de légitimité invite donc à un examen de proportionnalité. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées.

Les intérêts en jeu à prendre en considération sont, bien sûr, ceux de la personne concernée par les données, mais sont aussi, le cas échéant, l'intérêt de la société dans son ensemble. En résumé, pour être légitime, une finalité ne peut causer un préjudice plus grand à l'ensemble des intérêts en jeu que l'intérêt que représente le traitement.

Les décisions de jurisprudence reprises ci-dessous illustrent des hypothèses où un traitement de données a été ou non jugé comme légitime, car causant une atteinte admissible ou disproportionnée aux droits et intérêts des personnes concernées.

À l'occasion de l'affaire *Nice people* qui concernait une pratique de marketing viral développée par un site de rencontres en vue de se procurer d'importants revenus publicitaires, la Cour d'appel de Liège a été amenée à effectuer la mise en balance des intérêts et droits en présence pour vérifier la bonne application de l'article 5, f), de la loi vie

[30] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information: balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, p. 157.

[31] M.-H. BOULANGER, C. DE TERWANGNE et Th. LÉONARD, « La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », *J.T.*, 1993, pp. 377 et 379; M.-H. BOULANGER, C. DE TERWANGNE, Th. LÉONARD, S. LOUVEAUX, D. MOREAUX et Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 145; J. DUMORTIER et F. ROBBEN, note sous Prés. Comm. Anvers, 7 juillet 1994, et Prés. Comm. Bruxelles, 15 septembre 1994, *Computerr.*, 1994, pp. 244 et s.; S. GUTWIRTH, « De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.*, 1993/4, pp. 1409 et s.; Th. LÉONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », *in* F. RIGAUX, *La vie privée, une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.

privée[32]. « Le recours à cette disposition impose une balance des intérêts en présence, à savoir ceux du responsable du traitement et ceux de la personne concernée ». La Cour d'appel de Liège estima que « s'il peut être admis que les finalités de promotion et de prospection commerciale sont légitimes, elles sont néanmoins primées par les droits fondamentaux de la personne concernée, dont le droit à la protection de sa vie privée »[33].

La Cour d'appel de Gand[34] a été saisie d'une affaire dans laquelle la preuve d'un vol était apportée au moyen d'images issues d'une vidéo réalisée par une caméra de surveillance visible, accrochée sur la façade extérieure d'un bâtiment de la Banque nationale. Les personnes se trouvant sur le trottoir devant la Banque nationale étaient filmées par cette caméra. La banque réalisait ces prises de vues afin de prévenir et d'établir les atteintes à sa sécurité. La Cour d'appel estima que la licéité du traitement devait être jugée en application du principe de proportionnalité : l'intérêt général ou les intérêts légitimes du responsable de traitement doivent primer le droit à la protection de la vie privée de la personne concernée. Dans le cas d'espèce, la Cour a pris en compte dans son analyse le droit à l'inviolabilité du domicile (article 8 CEDH), le droit de propriété (article 544 C. civ.) et la loi du 10 avril 1990 réglementant la sécurité privée et particulière. Elle a jugé que, dans le cas soumis à son jugement, l'intérêt et les droits fondamentaux de la personne concernée ne pesaient pas plus lourd dans la balance et que le traitement poursuivait en conséquence une finalité légitime.

Une autre affaire mettait en cause la diffusion des informations commerciales de la banque de données « Creditel ». Parmi les informations à fournir au sujet d'une société figuraient les mandats antérieurs exercés par ses administrateurs. Le Tribunal de commerce de Courtrai fut appelé à se prononcer sur la légitimité de ce traitement de diffusion de données. Pour effectuer la mise en balance des intérêts en présence, le Tribunal a pris en compte, d'une part, la pertinence de l'information pour celui qui la traite et, d'autre part, la nature de cette information. D'après le tribunal, le caractère public des données doit également être pris en compte dans la réalisation de cette mise en balance. Le traitement fut considéré comme légitime[35].

La Cour constitutionnelle a été saisie d'une requête en annulation contre la loi du 21 janvier 2010 modifiant la loi du 25 juin 1992 sur le contrat d'assurance terrestre en ce qui concerne les assurances du solde restant dû pour les personnes présentant un risque de santé accru. En vertu de cette loi, la Commission des assurances devait établir un code de bonne conduite à défaut de quoi le Roi était habilité à régler la question des questionnaires médicaux dans le cadre des assurances du solde restant dû pour les personnes présentant un risque de santé accru. Dans son arrêt du 10 novembre 2011,

[32] Liège (7e ch.), 19 novembre 2009, *D.A.-O.R.*, 2010/96, p. 455. Voy. égal. « Chronique de jurisprudence », *R.D.T.I.*, n° 48 49/2012.

[33] *Ibid.*

[34] Gand, 28 mars 2002, *T. Strafr.*, 2002, pp. 326 à 334.

[35] Comm. Courtrai (1re ch.) 19 juin 2003, *T.G.R.-T.W.V.R.*, 2007, liv. 2, p. 100, confirmé par Gand, 6 janvier 2005, *T.G.R.-T.W.V.R.*, liv. 2, 2007, pp. 92 et 93.

la Cour a déclaré que « le législateur a pu estimer que l'utilisation de ces questionnaires devait être réglementée afin d'éviter que, dans le cadre de la conclusion d'un contrat d'assurance, des questions qui ne sont pas pertinentes ou qui sont excessives soient posées et qu'il soit ainsi porté atteinte de manière disproportionnée au droit au respect de la vie privée des intéressés. Il a également pu estimer que le fait que les assureurs exigent un examen médical complémentaire et demandent les résultats de celui-ci, en plus de l'utilisation d'un questionnaire médical, pouvait constituer une restriction disproportionnée du droit au respect de la vie privée de l'intéressé dans les cas où le montant assuré demeure limité »[36].

2. *Utilisations compatibles*

Après avoir spécifié que les données à caractère personnel doivent être collectées pour une ou plusieurs finalités déterminées, explicites et légitimes, la loi dispose que les données ne peuvent pas « être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables »[37]. Une fois qu'on a collecté des données à caractère personnel, on ne peut faire n'importe quoi avec ces données. Seules les utilisations compatibles avec la ou les finalités déterminées et annoncées au départ, au moment de la collecte, sont admises.

Pour savoir si une utilisation est compatible avec la finalité de collecte des données, il faut tenir compte notamment des prévisions raisonnables des personnes concernées. Si l'utilisation envisagée offre un lien logique avec la finalité annoncée, les personnes concernées peuvent raisonnablement s'attendre à ce qu'une telle utilisation ait lieu. Elle sera donc jugée compatible et sera, dès lors, légale[38].

La loi propose également comme critère de compatibilité le fait que le traitement soit prévu par des dispositions légales ou réglementaires. Pour être retenues comme légitimant des opérations effectuées sur des données, les dispositions légales ou réglementaires doivent être accessibles et surtout prévisibles, selon le prescrit de l'article 8, § 2, CEDH. L'exigence de prévisibilité impose que la norme soit rédigée avec suffisamment de précision. À sa lecture, les personnes concernées doivent comprendre qu'un traitement sera opéré sur des données les concernant qui avaient été collectées dans un but initial différent de celui poursuivi par ce traitement ultérieur.

À titre d'exemple d'utilisations des données qui ne sont pas compatibles, on citera le cas d'une banque ayant également des activités d'assurance, qui identifie dans les virements effectués par ses clients ceux qui paient des primes d'assurance plus élevées que les primes de ses produits d'assurance et qui leur envoie un courrier les invitant sur

[36] C. const., 10 novembre 2011, n° 166/2011, B.16.7.

[37] Article 4, § 1er, 2°, de la loi du 8 décembre 1992.

[38] Le RGPD présente, à son article 6, § 4, une série de critères permettant d'établir si la nouvelle finalité du traitement est compatible ou non avec la finalité de la collecte de départicle Il s'agit du lien pouvant exister entre les deux finalités, du contexte, de la nature des données, des conséquences du traitement ultérieur et des garanties existantes.

cette base à changer de compagnie d'assurances. Cette pratique a été condamnée par les tribunaux[39].

C'est également un problème de compatibilité qui a été mis en exergue par les velléités d'une banque néerlandaise ayant fait grand bruit en mars 2014. Cette banque révéla son intention d'exploiter les masses de données amoncelées dans ses ordinateurs et réseaux internes pour développer une stratégie *Big data* aux fins de réaliser un ciblage ultra affiné de ses clients et de leur adresser des offres promotionnelles de sociétés tierces. Cette annonce provoqua un tollé immédiat « dans les médias et parmi les associations de consommateurs, la banque usurpant selon eux ses droits sur la confidentialité des données personnelles en les vendant »[40]. Il est clair que cette pratique ne pouvait passer pour compatible avec les finalités des traitements classiques d'une banque.

C'est pourtant aujourd'hui l'ensemble du secteur qui rumine des projets d'utilisation de leurs trésors de données personnelles à des fins commerciales, bien au-delà des nécessités des services financiers offerts[41]. Le RGPD offrira un cadre juridique à ces perspectives étant donné qu'il admet expressément que l'on traite des données pour une finalité incompatible avec la finalité initiale du traitement, mais seulement dans deux hypothèses : avec le consentement (libre, éclairé, spécifique et indubitable) des personnes concernées ou lorsque c'est fondé sur le droit de l'Union ou le droit d'un État membre visant à garantir un des objectifs énumérés à l'article 23, paragraphe 1er, du règlement.

3. *Données adéquates et pertinentes au regard de la finalité*

Afin de respecter le principe de finalité, il convient par ailleurs de bien sélectionner les données à caractère personnel qui vont faire l'objet d'un traitement. Seules peuvent être traitées les données adéquates et pertinentes au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement[42]. Pour être jugées pertinentes, les données doivent présenter un lien nécessaire et suffisant avec les finalités poursuivies[43].

[39] Anvers, 3 mai 1999, *Ann. prat. comm.*, 1999, pp. 524 à 527 ; *A.J.T.*, 1999, p. 437, note C. De Vos ; Prés. Comm. Anvers, 7 juillet 1994, *D.C.C.R.*, 1994-1995, p. 77, note Th. Léonard.

[40] M. Leblanc-Wohrer, « Le défi de la protection des données personnelles », *L'AGEFI Hebdo*, 5 juin 2014, www.agefi.fr/banque-assurance/actualites/hebdo/20160210/defi-protection-donnees-personnelles-154345.

[41] H. Stefani, « Le Big Data au service d'une connaissance client affinée », *Revue-Banque.fr*, 25 février 2014, www.revue-banque.fr/management-fonctions-supports/article/big-data-au-service-une-connaissance-client-affine ; Ch. Lejoux, « Le big data, un enjeu crucial pour le secteur bancaire », *La Tribune*, 28 janvier 2016, www.latribune.fr/entreprises-finance/banques-finance/banque/le-big-data-un-enjeu-crucial-pour-le-secteur-bancaire-545979.html ; Ph. Gelis, « Le "Big Data"... L'arme secrète des banques pour gagner plus », Frenchweb.fr, 22 janvier 2016, www.frenchweb.fr/le-big-data-larme-secrete-des-banques-pour-gagner-plus/224205#LwJh6OY7PyK6CFfy.99.

[42] Les données ne peuvent pas non plus être excessives, mais cette caractéristique correspond au principe de proportionnalité et sera vue *infra*, sous le point consacré à ce principe.

[43] M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreaux et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 146.

De nombreux formulaires, jugés à l'aune de cette exigence de pertinence des données, devraient bien être allégés en termes de données recueillies.

4. Conservation des données limitée au regard de la finalité

La détermination de la finalité permet également de définir la durée de conservation des données dès lors que l'article 4, § 1er, 5°, de la loi vie privée prescrit que les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement [...] ».

La durée licite de conservation des données n'est donc pas uniforme, mais dépend de la finalité du traitement des données, sous réserve des précisions apportées par l'arrêté royal du 13 février 2001 concernant la conservation de données « au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques »[44].

Dès l'instant où les données ne sont plus nécessaires pour atteindre la finalité de leur collecte ou les finalités ultérieures compatibles, le responsable du traitement est tenu soit de les effacer, soit de les anonymiser, c'est-à-dire de faire disparaître irréversiblement leur élément identifiant[45]. Le responsable du traitement doit faire cette opération de suppression ou d'anonymisation des données spontanément, et non sur demande des personnes concernées.

Il est à noter toutefois que les données peuvent être conservées à des fins probatoires durant une période correspondant au délai de prescription.

C. Le principe de proportionnalité

1. Proportionnalité du traitement

L'article 5 de la loi du 8 décembre 1992[46] énonce les six seules hypothèses dans lesquelles un traitement de données peut être effectué. « Ces hypothèses représentent en fait les situations dans lesquelles l'équilibre des intérêts en présence est *a priori* atteint »[47]. M.-H. Boulanger, intervenant au nom de la Commission de la protection de la vie privée, signala, lors des discussions qui accompagnèrent le vote de la modification de

[44] Article 4, § 1er, 4°, de la loi du 8 décembre 1992.

[45] Rappelons qu'il ne suffit pas de coder les données pour les anonymiser. Des données codées demeurent des données à caractère personnel tant que la clé du code est conservée (voy. *supra*).

[46] Reproduction de l'article 7 de la directive 95/46 du 24 octobre 1995.

[47] C. DE TERWANGNE, « La nouvelle loi belge de protection des données à caractère personnel », *in* P. TABATONI (dir.), *La protection de la vie privée dans la société d'information*, Cahier des Sciences morales et politiques, Paris, PUF, 2002, p. 99, disponible sur le site de l'Académie des Sciences morales et politiques, www.asmp.fr/travaux/gpw_internetvieprivee.htm. Dans le même sens, J. DHONT, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 1/2000, pp. 323 et 324.

la loi belge, que les situations visées par l'article 5 de la loi créent « une présomption d'équilibre d'intérêts »[48].

Les articles 4, § 1er, b), et 5, doivent être lus conjointement. Le fait de se trouver dans une des situations énoncées à l'article 5 n'implique pas que l'exigence de finalité légitime de l'article 4 soit *ipso facto* rencontrée. Les hypothèses visées dans la première disposition n'empêchent pas un contrôle sur la base de la deuxième[49]. En fait, on peut considérer que l'article 5 prévoit des situations abstraites dans lesquelles l'équilibre des intérêts en présence est normalement respecté, sans préjudice d'un contrôle concret, sur la base de l'article 4, permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu[50]. Ce n'est pas parce qu'on a le consentement d'une personne à ce que l'on traite les données la concernant (ce qui correspond à une des hypothèses de légitimité de l'article 5) que le traitement est d'office admissible. Il porte peut-être atteinte de manière disproportionnée à un intérêt collectif qui n'a forcément pas été pris en compte par la personne concernée qui n'a envisagé, comme il se doit, que ses propres droits et intérêts pour donner son consentement. La condition de finalité légitime de l'article 4, § 1er, b), n'est, dans ce cas, pas rencontrée alors même que l'article 5 est respecté. Le traitement de données envisagé doit être déclaré illégal.

Pour être admis, tout traitement de données doit donc respecter le principe de proportionnalité et reposer sur un fondement légitime, c'est-à-dire correspondre à l'une des six hypothèses énoncées par la loi. Les hypothèses pertinentes dans le contexte des activités des institutions financières sont les suivantes.

- La personne concernée a sans ambiguïté donné son *consentement*[51]. Le consentement n'est valable que s'il est libre (c'est-à-dire s'il a été émis sans pression), spécifique (le consentement doit porter sur un traitement de données précis ; il ne peut être général) et informé (la personne a reçu toute l'information utile sur le traitement envisagé ; elle doit notamment savoir qui utilisera ses données et pourquoi, et se rendre compte des destinataires de ses données). Le consentement ne doit pas nécessairement être donné par écrit, mais alors se pose un problème de preuve à charge du responsable.
- Le traitement des données est nécessaire à l'exécution d'un *contrat* ou à l'exécution de mesures précontractuelles sollicitées par la personne concernée. C'est le cas de l'enregistrement de données pour établir un contrat d'ouverture de compte, pour permettre la facturation d'un service ou pour octroyer un crédit, etc. Il faut que le traitement de données soit véritablement *nécessaire* à l'exécution du contrat en question ou des mesures précontractuelles. Ainsi, la mise en

[48] Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Chambre, 1998-1999, n° 1566/10, p. 47.

[49] M. VAN OVERSTRAETEN et S. DEPRE, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 689 et 690.

[50] M.-H. BOULANGER, C. DE TERWANGNE, Th. LÉONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *op. cit.*, p. 148, n° 41 ; J. DHONT, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 1/2000, pp. 324 et 325.

[51] Article 5, alinéa 1er, littera a, de la loi du 8 décembre 1992.

place de caméras de surveillance dans les différentes zones d'une banque ne peut être jugée nécessaire à l'exécution des contrats liant la banque à ses clients. Ces opérations ne sont pas illégales pour autant, mais, pour être admissibles, elles doivent s'appuyer sur un autre fondement légitime que l'exécution du contrat (la balance d'intérêts dans ce cas, voy. *infra*).

- Le traitement est exigé par une loi, un décret ou une ordonnance. De nombreuses collectes d'informations qui doivent être réalisées au sein des banques entrent dans cette hypothèse. Le secteur bancaire et financier est en effet intensément soumis à des obligations légales visant notamment à lutter contre le blanchiment d'argent et le financement du terrorisme et instaurant une obligation de vigilance à l'égard des clients[52], qui se traduit par le fameux K.Y.C. (*know your customer*), ou visant à garantir l'adéquation du produit ou service financier proposé à la situation et au profil du client (directive « MiFID », *Markets in Financial Instruments Directive* – directive concernant les marchés d'instruments financiers[53]) et impliquant dès lors la récolte d'une série d'informations sur chaque client.
- Le traitement des données est « nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée »[54]. Cette dernière hypothèse correspond à une mise en balance des intérêts et droits en présence. Il revient dans un premier temps au responsable du traitement d'effectuer lui-même la mise en balance et, s'il estime que la mise en œuvre du traitement de données qu'il envisage sert un intérêt supérieur à celui de la personne concernée ainsi qu'aux droits et libertés de celle-ci, il conclura que son traitement est légitime. La personne concernée pourra, quant à elle, contester le résultat de cette mise en balance et estimer que ses intérêts, droits et libertés prévalent sur l'intérêt poursuivi par le responsable. La loi lui octroie pour ce faire un droit d'opposition (voy. *infra*). En dernier ressort, si les deux intervenants ne se mettent pas d'accord à la suite d'une opposition manifestée par la personne concernée, ils pourront s'adresser à la Commission de la protection de la vie privée voire au tribunal.

[52] Loi du 18 janvier 2010 modifiant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et le Code des sociétés.

[53] Directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers (MiFID), modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil, J.O., L 145 du 30 avril 2004, p. 144; transposée en droit belge par la loi du 22 mars 2006 relative à l'intermédiation en services bancaires et en services d'investissement et à la distribution d'instruments, et par les articles 162 à 181 de la loi-programme du 27 avril 2007 modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

[54] Article 5, alinéa 1er, littera e, de la loi du 8 décembre 1992.

2. *Proportionnalité des données*

L'article 4, 3°, de la loi vie privée prescrit qu'outre d'être adéquates et pertinentes ainsi que cela a été mentionné antérieurement, les données à caractère personnel doivent être « non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

Cela signifie que « [d]es données pertinentes au regard de l'objectif poursuivi, mais induisant une atteinte excessive à la personne concernée par rapport à l'intérêt qu'elles présentent pour la personne qui souhaite les traiter, ne peuvent être recueillies »[55]. En outre, le responsable de traitement ne pourra pas collecter des données qui ne seraient pas nécessaires pour atteindre la finalité qu'il a préalablement déterminée, dans la mesure où moins de données ou des données moins attentatoires à la personne concernée permettent d'atteindre cette finalité.

D. La qualité des données

En vertu de l'article 4, § 2, de la loi vie privée, il incombe au responsable du traitement de veiller à la qualité des données à caractère personnel traitées.

On a déjà vu dans les points précédents consacrés aux principes de finalité et de proportionnalité qu'aux termes de l'article 4, § 1er, 3°, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

Les données traitées doivent, en outre, être exactes et, si nécessaire, mises à jour.

Le responsable du traitement devra « faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8 »[56]. Il incombe donc au responsable du traitement de prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités poursuivies, soient effacées ou rectifiées. C'est une obligation de moyens et non de résultat qui est mise à charge du responsable.

On attire l'attention sur le fait qu'il ne peut être question de caractère exact ou inexact d'informations subjectives tels les avis ou opinions. On ne peut donc contester l'exactitude de telles informations. Toutefois, il importe que l'opinion émise s'appuie sur des données objectives dont l'éventuelle inexactitude pourra, elle, être mise en question.

À titre d'illustration de cette obligation de diligence concernant la qualité des données, il a été jugé en matière de crédit que le prêteur qui fournit des informations à l'UPC (Union professionnelle du crédit, association professionnelle représentative du secteur du crédit aux particuliers) et à la Banque nationale est responsable d'un traitement

[55] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *in Cabinet d'avocats et technologies de l'information: balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005 p. 162.

[56] Article 16, § 2, 1°, de la loi du 8 décembre 1992.

de données ; c'est donc à lui « qu'il incombe de s'assurer que sont remplies toutes les conditions auxquelles la transmission du nom des débiteurs défaillants à l'UPC et à la Banque nationale est subordonnée ». En transmettant une information inexacte, le prêteur a été jugé comme ayant commis une faute consistant en un manquement à l'obligation générale de prudence et diligence qui s'impose à tous[57].

IV. Les données sensibles

Certaines informations personnelles sont par nature beaucoup plus sensibles que d'autres. Alors que le nom et l'adresse de quelqu'un sont des informations somme toute anodines, il n'en est pas de même des convictions politiques de cette personne, de sa santé ou de son passé judiciaire.

L'identification d'une catégorie particulière de données à caractère personnel auxquelles on réserve une protection plus élevée est liée aux risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données qui justifie le traitement différencié qui leur est accordé[58]. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime des sujets de données ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée.

La catégorie des données qualifiées de « sensibles » est visée par les articles 6, 7 et 8 de la loi vie privée, qui réservent un régime plus protecteur à ces données. Ces données rassemblent en fait trois sous-catégories de données :

- les données à caractère personnel « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, et les données relatives à la vie sexuelle », données qualifiées de sensibles au sens strict (visées par l'article 6 de la loi)[59] ;
- les données relatives à la santé (visées à l'article 7 de la loi) ; et
- les données à caractère personnel « relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté », communément reprises sous l'appellation de « données judiciaires » (visées à l'article 8 de la loi).

Des données de ces trois sous-catégories se retrouvent dans la masse de données gérées par les institutions financières et peuvent concerner tant les responsables de l'institution que le personnel ou les clients.

[57] Civ. Bruxelles (72e ch.), 15 octobre 2003, *J.T.*, 2004, pp. 140 et 141.

[58] Voy. J. RINGELHEIM, « Recueil des données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in Les nouvelles lois luttant contre la discrimination*, Bruges, la Charte, 2008, pp. 91 et s.

[59] Le RGPD ajoute à la liste les « données génétiques » et les « données biométriques [traitées] aux fins d'identifier une personne physique de manière unique » (article 9, § 1er, RGPD).

A. Des données interdites...

Il est en principe interdit de collecter, d'enregistrer, d'utiliser ou de communiquer des données telles que celles énumérées ci-dessus. Celui qui le fait s'expose à une amende et, en cas de récidive, à un emprisonnement de trois mois à deux ans.

B. ... sauf dans certains cas très spécifiques

On peut tout de même traiter ces données dans certains cas bien déterminés.

À l'exception des données relatives à des suspicions, des poursuites et des condamnations, les données sensibles peuvent être traitées avec le *consentement écrit* de la personne concernée. Cette exception n'est toutefois pas valable lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement l'empêchant de refuser librement son consentement. Dans une telle situation, le consentement écrit est tout de même admis s'il permet d'octroyer un avantage à la personne concernée.

On peut également traiter ces données si le traitement est exigé par la législation sur le travail ; s'il porte sur des données manifestement rendues publiques par la personne concernée (par exemple, l'appartenance politique d'une personne ayant mené une campagne électorale) ; s'il est nécessaire en vue de l'application de la sécurité sociale ; ou s'il est rendu obligatoire par une norme législative pour un motif important d'intérêt public, etc.

Les données relatives aux suspicions, poursuites et condamnations peuvent être traitées par un avocat pour la défense de ses clients ; par quiconque pour la gestion de son propre contentieux ; ou, si c'est nécessaire, à la réalisation de finalités fixées par la loi.

C. Des garanties supplémentaires

Pour toutes ces hypothèses, des garanties supplémentaires sont à respecter[60], notamment :

- le responsable du traitement doit désigner les catégories de personnes ayant accès aux données et décrire de manière précise leur fonction par rapport au traitement des données. Cela n'oblige pas le responsable du traitement à désigner les personnes par leur nom, mais plutôt à établir des profils d'accès (les médecins et infirmières de l'hôpital, par exemple) ;
- lors de l'information de la personne concernée (voy. le point II, D, 1. « Détermination du responsable du traitement » *supra*), le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement des données.

[60] Voy. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, p. 459.

Cela permet de contrôler sur quoi il se base pour traiter des données en principe interdites ;

- enfin, lorsqu'on se fonde sur le consentement écrit d'une personne pour traiter ses données sensibles, il faut signaler à cette personne les motifs pour lesquels ces données sont traitées et lui communiquer la liste des catégories de personnes ayant accès aux données.

Par ailleurs, une garantie particulière a été prévue par le législateur pour les traitements de données relatives à la santé. Ces traitements doivent impérativement être effectués sous la responsabilité d'un professionnel des soins de santé qui sera, ainsi que ses préposés ou mandataires, tenu au secret. Il n'y a que dans quelques cas, dont celui d'un consentement écrit de la personne concernée, que cette exigence ne doit pas être rencontrée. La notion de « professionnel des soins de santé » est définie par l'arrêté royal n° 78 relatif à l'exercice des professions des soins de santé[61].

V. Les droits de la personne concernée

Toute personne, quels que soient son âge, son domicile (en Belgique, dans l'UE ou le reste du monde) ou sa nationalité (belge ou étrangère), se voit reconnaître des droits vis-à-vis de ceux qui traitent des données sur elle.

Les droits octroyés à la personne concernée visent en premier lieu à assurer la transparence des traitements de données. Cette transparence, d'initiative ou sur demande, doit permettre à la personne concernée non seulement d'avoir connaissance, mais aussi de contrôler ce qui est fait avec ses données, de vérifier le respect des règles, de traquer les abus ou les illégalités, de corriger les erreurs.

A. Le droit à l'information

Le traitement des données doit se faire dans la transparence, troisième grand principe de protection des données après le principe de finalité et celui de proportionnalité évoqués antérieurement. Il s'agit, dans un premier temps, pour le responsable du traitement, de fournir spontanément de l'information à la personne concernée à propos du traitement qui va être effectué avec les données la concernant. Ce droit pour l'un s'apparente donc à une obligation pour l'autre. Le droit à l'information est présenté en détail sous son aspect d'obligation de fournir des informations à la personne concernée dans le chapitre consacré aux obligations du responsable du traitement (voy. *infra*).

[61] Arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé (intitulé modifié par l'article 27 de la loi du 10 août 2001 portant des mesures en matière de soins de santé).

B. Le droit d'accès

Le droit d'accès offre à la personne concernée une autre voie pour obtenir des informations sur les traitements effectués sur ses données. Cette voie exige une démarche de la part de la personne concernée.

1. Le droit d'obtenir des informations sur le traitement des données et sur les communications effectuées

En vertu de l'article 10, § 1er, alinéa 1er, a), de la loi vie privée, chacun a le droit d'interroger tout responsable de traitement de données à caractère personnel pour savoir s'il détient ou non des données sur lui. Le responsable interrogé doit confirmer ou non s'il détient des données à propos de l'individu qui s'est adressé à lui et, si c'est le cas, il doit fournir des indications sur le sort réservé à ces données. Il doit à tout le moins éclairer la personne concernée sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées.

Le droit d'être informé des destinataires ou des catégories de destinataires à qui les données sont communiquées ainsi que du contenu des communications soulève la question de la portée dans le temps de ce type d'information. En effet, c'est souvent parce que l'on s'est rendu compte de quelque chose de douteux ou parce que l'on souhaite savoir à quelle source des personnes ont obtenu des informations que l'on exerce son droit d'accès pour découvrir les personnes à qui les données ont été transmises. L'accès aux données sur les destinataires est aujourd'hui, dans un monde numérisé, lié à la question de l'accès aux *log files* ou journaux d'événements. Ces derniers sont des fichiers qui relèvent un certain nombre de renseignements sur toutes les transactions gérées par le serveur. C'est donc à partir de ces journaux et des traces digitales qu'ils conservent que l'on peut identifier les accès qui se sont produits. L'information sur les destinataires se heurte toutefois directement aux pratiques d'effacement de telles données au terme d'un certain délai.

Saisie d'une affaire mettant en cause un citoyen néerlandais désireux de connaître les personnes à qui ses données détenues par la commune avaient été communiquées, mais qui s'était heurté à une impossibilité d'être éclairé au-delà d'un an en raison de l'effacement de ce type de données, la Cour de justice de l'Union européenne[62] a affirmé que le sens même du droit d'accès dans toutes ses composantes est de permettre aux individus de prendre connaissance du sort réservé à leurs données et de procéder à des vérifications des opérations effectuées sur elles, afin d'être à même d'exercer leurs autres droits prévus par la directive. En conséquence, pour la Cour, il est impératif que l'accès ne soit pas réduit au présent, mais couvre également le passé.

[62] C.J.C.E., arrêt *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, 7 mai 2009, C-553/07. Voy. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, nos 48 et 49, 2012, pp. 95 et 96.

Il ne s'agit pas pour autant de permettre de remonter sans limites dans le temps, ce qui induirait une obligation corrélative pour les responsables de conserver indéfiniment les informations relatives aux actions réalisées avec les données, en l'occurrence aux communications des données. La fixation d'un délai de conservation légitime varie en fonction de paramètres identifiés par la Cour et doit être tempérée par l'intervention du critère de proportionnalité. Les paramètres à prendre en considération sont les suivants : la durée de conservation des données à caractère personnel « de base » ou « principales », c'est-à-dire celles qui font l'objet du traitement et dont les données relatives aux destinataires peuvent être considérées comme « accessoires » (en cas de très longue durée de conservation des données principales, l'intérêt de l'accès peut s'estomper au fil du temps, mais la durée de conservation des traces des communications doit tout de même demeurer dans un juste rapport de proportionnalité avec la durée de conservation des données principales), les délais de recours, la nature plus ou moins sensible des données principales, le nombre des destinataires et la fréquence des communications[63].

L'arrêt *Rijkeboer* présente un enseignement concret pour les responsables de traitement. Ils savent à l'avenir que découle de la directive (et dès lors des lois nationales qui l'ont transposée) l'obligation de veiller à la conservation des traces des communications et accès aux données accordés à des tiers pendant à tout le moins une durée raisonnable, afin de permettre aux personnes concernées d'être informées, à leur demande, de ces transmissions de leurs données et de pouvoir en contrôler la licéité[64].

2. *L'accès aux données à caractère personnel traitées*

Aux termes de l'article 10, § 1er, alinéa 1er, b), de la loi vie privée, la personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet du traitement. C'est l'ensemble des données traitées qui doivent être communiquées, tant les données objectives que les données subjectives (par exemple, avis ou évaluation de la solvabilité d'une personne).

L'exigence que les données soient communiquées sous une forme intelligible implique que la forme des données doit permettre à un individu ordinaire de saisir la portée de l'information transmise. Ainsi, si un code ou un profil particulier est attribué à la personne concernée (par une banque qui évalue sa valeur de crédit, par exemple, ou à l'issue de tests d'embauche), celle-ci doit être mise en mesure de comprendre la signification du code ou du profil.

[63] Voy. les paragraphes 58 et 59 et 63 de l'arrêt et leur commentaire dans C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E, 7 mai 2009, *R.D.T.I.*, 2011, n° 43, pp. 65 à 81.

[64] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*

3. *L'accès à l'information sur l'origine des données*

L'article 10, § 1er, alinéa 1er, b), de la loi vie privée garantit aussi à toute personne concernée le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, de toute information disponible sur l'origine des données.

Cette obligation d'information sur l'origine des données, qui est logiquement d'application lorsque les données n'ont pas été recueillies directement auprès de la personne concernée, est d'un grand intérêt étant donné que c'est souvent la question de la source des informations qui préoccupe les personnes concernées (comment se fait-il que mes informations se retrouvent dans les mains de cet organisme, qui les lui a fournies ?).

Enfin, en cas de problèmes liés à la qualité des données et de nécessité de correction, il devient possible de faire effectuer ces corrections à la source, ce qui évite la propagation ultérieure d'erreurs.

4. *L'accès à la logique qui sous-tend le traitement des données*

Lorsqu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, cette personne doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui sous-tend le traitement automatisé en question[65].

Le but de ce droit d'accéder à la logique d'un traitement (c'est-à-dire au raisonnement, aux critères appliqués) consiste à permettre aux personnes concernées de contrôler les fondements de décisions prises à leur encontre, impliquant le traitement de leurs données. Ce droit présente un grand intérêt face au déploiement exponentiel du phénomène de profilage.

5. *Modalités d'exercice du droit d'accès*

Pour exercer son droit d'accès, la personne concernée doit adresser une demande datée et signée au responsable du traitement. La personne concernée soit remet la demande sur place, soit l'envoie par la poste (l'exigence d'un pli recommandé a été supprimée) ou par tout moyen de télécommunication[66]. Ceci implique que les demandes pourront, par exemple, être introduites par courrier électronique, mais seulement accompagnées d'une signature électronique considérée comme juridiquement équivalente à la signature manuscrite ou du scan de la carte d'identité.

Le responsable du traitement doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande[67].

[65] Article 10, § 1er, alinéa 1er, c), de la loi du 8 décembre 1992.

[66] Article 32 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

[67] Article 10, § 1er, alinéa 3, de la loi du 8 décembre 1992.

C. Le droit de rectification et d'effacement/le droit à l'oubli

Toute personne concernée peut, sans frais, faire rectifier les données à caractère personnel inexactes qui se rapportent à elle et faire effacer ou interdire d'utilisation les données incomplètes ou non pertinentes au regard de la finalité du traitement ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui ont été conservées au-delà de la période autorisée[68]. Ce droit d'effacement est présenté, dans le RGPD, comme assimilé au « droit à l'oubli », notion qui a fait couler beaucoup d'encre et suscité de nombreux débats[69].

Dans le mois qui suit l'introduction de la demande de rectification ou d'effacement, le responsable du traitement communique à la personne concernée les rectifications ou effacements des données qu'il a effectués.

Dès la réception de la demande tendant à faire rectifier, supprimer ou interdire d'utiliser ou de divulguer des données à caractère personnel, et jusqu'à ce qu'une décision soit coulée en force de chose jugée, le responsable du traitement doit indiquer clairement, lors de toute communication d'une donnée à caractère personnel, que celle-ci est contestée[70].

Les demandes de rectification, de suppression et d'interdiction de traitement des données fondées sur l'article 12 de la loi se font selon la même procédure et auprès des mêmes personnes que ce qui est prévu pour l'exercice du droit d'accès.

Si des données inexactes, incomplètes ou non pertinentes ont été transmises à des tiers ou au public, le responsable doit, dans le mois qui suit l'introduction d'une requête en rectification portant sur ces données, communiquer les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées. Le responsable est cependant libéré de cette obligation lorsqu'il n'a plus connaissance des destinataires de la communication ou lorsque la notification paraît impossible ou implique des efforts disproportionnés[71].

D. Le droit d'opposition

En vertu de l'article 12, § 1er, alinéas 2 et 3, de la loi vie privée, toute personne a le droit de s'opposer à ce que les données la concernant fassent l'objet d'un traitement, pourvu qu'elle invoque des raisons sérieuses et légitimes tenant à sa situation particulière.

[68] Article 12, § 1er, alinéas 1er et 5, de la loi du 8 décembre 1992.

[69] Voy. C. DE TERWANGNE, « The Right to be Forgotten and the Informational Autonomy in the Digital Environment », *The Ethics of Memory in a Digital Age: Interrogating the Right to Be Forgotten*, Palgrave, octobre 2014, pp. 82 à 101; C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *in Les enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 237 à 268.

[70] Article 15 de la loi du 8 décembre 1992.

[71] Article 12, § 3, de la loi du 8 décembre 1992.

Il est à noter que le RGPD apportera une nuance de taille dans l'exercice du droit d'opposition, étant donné que ce sera au responsable du traitement à démontrer « qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice », faute de quoi, le responsable ne pourra plus traiter les données en cause[72].

Le droit d'opposition n'est pas reconnu pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat. De même, lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire, les personnes concernées ne peuvent s'opposer au traitement.

Lorsque les données sont collectées à des fins de *direct marketing*, la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement projeté de données à caractère personnel la concernant.

En cas d'opposition au traitement de données à caractère personnel par la personne concernée, le responsable du traitement communique à cette dernière, dans le mois qui suit l'introduction de sa demande, quelle suite il a donnée à sa requête[73].

E. Le droit de ne pas être soumis à une décision automatisée

L'homme ne doit pas être soumis à la machine. Au nom de la dignité humaine, il est inadmissible qu'une décision qui s'impose à un individu dépende des seules conclusions d'une machine.

À l'exemple de la directive 95/46 qui a traduit cette conviction dans son article 15[74], l'article 12*bis* de la loi belge interdit qu'une décision individuelle produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.

Ce principe est crucial aujourd'hui alors que la technique est de plus en plus souvent utilisée pour s'en remettre à un « ordinateur » et aux algorithmes qu'il applique pour décider du traitement à réserver à un individu (le considérer ou non comme fraudeur fiscal ou comme cible de marketing, par exemple). Les décisions affectant de manière significative les individus (par exemple, la décision de refuser d'octroyer un prêt; de soumettre une personne à une surveillance intrusive, etc.) sont de plus en plus souvent motivées « par le fait que l'ordinateur a dit non », alors même que les personnes « responsables » de la décision ne comprennent pas nécessairement le calcul ou raisonne-

[72] Article 21, § 1er, RGPD.

[73] Article 12, § 3, alinéa 2, de la loi du 8 décembre 1992.

[74] Voy. l'analyse de cette disposition par L. BYGRAVE, « Minding the machine: Article 15 of the EC Data Protection Directive and automated profiling », *C.L.S.R.*, 2001, vol. 17, pp. 17 à 24.

ment appliqué par la machine à un ensemble de données pour aboutir à la conclusion énoncée[75].

Une telle interdiction doit bien évidemment connaître des limitations ou exceptions là où cela se justifie en considération du contexte et des risques en jeu. Ainsi, dans le monde commercial, il est courant de recourir à des évaluations automatisées du profil du consommateur lorsqu'il s'agit de contrats d'octroi de prêt ou de souscription d'une assurance. Le recours à la technique du profilage déborde désormais largement ces contextes commerciaux restreints et se nourrit de quantités impressionnantes de données glanées de toutes parts.

L'article 12*bis* prévoit que l'interdiction de soumettre un individu à une décision entièrement automatisée ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Pour être admissibles, ces exceptions doivent toutefois être accompagnées de mesures garantissant la sauvegarde de la dignité de l'homme face à la machine, c'est-à-dire la sauvegarde des intérêts légitimes de l'intéressé en prévoyant à tout le moins le droit pour l'intéressé de faire valoir *utilement* son point de vue. Le RGPD apporte des précisions supplémentaires en garantissant le « droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision »[76].

F. Un nouveau droit à venir : droit à la portabilité des données

Le RGPD garantit aux personnes concernées un nouveau droit : le droit à la portabilité des données. Aux termes de l'article 20, en cas de traitement automatisé de données fondé sur un contrat ou sur le consentement de la personne concernée, cette dernière a le droit de recevoir du responsable du traitement les données à caractère personnel qu'elle a fournies, « dans un format structuré, couramment utilisé et lisible par machine », afin de transmettre ces données à un autre responsable du traitement.

G. Les recours en cas de difficulté à faire respecter ses droits

Il est à noter qu'un recours juridictionnel spécifique a été mis en place par la loi du 8 décembre 1992[77]. Une possibilité d'action est ouverte auprès du président du tribunal de première instance siégeant comme en référé, afin de lui soumettre toute

[75] LRDP Kantor Ltd, en association avec Centre for Public Reform, *Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, Rapport final, Note de synthèse, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, p. 2.

[76] Article 22, § 3, RGPD.

[77] Article 14 de la loi du 8 décembre 1992.

demande concernant l'exercice des principaux droits garantis à la personne concernée (droit d'accès, droit de rectification et droit d'opposition).

Un recours devant les juridictions pénales est également envisageable en cas de non-respect des obligations liées au droit à l'information et au droit d'accès, étant donné que ce non-respect est sanctionné pénalement[78].

VI. Les obligations du responsable du traitement

Le propos se concentre ici sur les deux obligations principales, sans s'attarder à d'autres obligations comme la déclaration des traitements de données (qui va disparaître avec le RGPD, remplacée par un devoir de documentation interne) ou les obligations nouvelles à venir que sont la *Privacy by design* et la *Privacy by default* (protection des données dès la conception et protection des données par défaut).

A. Assurer la transparence du traitement de données : le devoir d'information

Après les principes de finalité et de proportionnalité, le troisième principe fondamental sur lequel repose la loi vie privée est celui de la transparence de tout traitement. Cette transparence s'exerce par le biais de l'obligation d'informer l'individu dont on traite les données et par le devoir de répondre à ses demandes d'accès aux données conservées (sur le droit d'accès, *cf. supra*).

Tout responsable de traitement de données à caractère personnel est tenu de fournir certaines informations aux personnes concernées par les données. Cette formalité doit être accomplie soit au moment de l'obtention des données, lorsque les données sont obtenues de la personne concernée elle-même, soit au plus tard au moment de la première communication des données, lorsque les données ont été obtenues de manière indirecte[79].

Les informations à fournir consistent dans :

- les coordonnées du responsable du traitement (nom et adresse),
- les finalités du traitement,
- l'existence du droit de s'opposer gratuitement au traitement envisagé à des fins de *direct marketing* (ce qui recouvre toutes démarches de promotion),
- les destinataires ou catégories de destinataires des données,
- l'existence d'un droit d'accès et de rectification des données,
- le caractère obligatoire ou non des réponses ainsi que les conséquences d'un défaut éventuel de réponse (lorsque les données sont collectées auprès de la personne concernée) et les catégories de données (lorsque les données sont obtenues de source indirecte).

[78] Article 39, 4° et 5°, de la loi du 8 décembre 1992.

[79] Article 9 de la loi du 8 décembre 1992.

Les quatre derniers types d'information à fournir ne doivent pas être communiqués si, compte tenu des circonstances particulières dans lesquelles le traitement est effectué, cela n'est pas nécessaire pour assurer un traitement loyal des données.

Les articles 13 et 14 du RGPD allongent la liste des informations à communiquer aux personnes concernées. Ainsi, des informations sur un éventuel délégué à la protection des données, sur la base juridique du traitement, sur les intérêts légitimes du responsable ou d'un tiers qui fondent le traitement, sur les destinataires des données et sur les intentions de transférer les données dans un pays tiers offrant ou non une protection adéquate, figurent dans la catégorie des informations à fournir obligatoirement. Dans les informations additionnelles à fournir pour garantir un traitement équitable et transparent apparaissent la période de conservation des données, des informations sur l'ensemble des droits, la source d'où proviennent les données (en cas de collecte indirecte des données) et, le cas échéant, l'existence d'une décision automatisée, y compris un profilage, accompagnée d'informations sur la logique sous-jacente.

Rappelons que, pour les données sensibles, celles relatives à la santé et les données judiciaires, des informations complémentaires doivent encore être données, ainsi que cela est prévu au chapitre III de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992.

Cette obligation d'information connaît certaines exceptions qui ne sont essentiellement valables que dans les hypothèses de collecte indirecte des données.

Le responsable du traitement de données est dispensé de fournir les informations requises dans l'hypothèse où cette démarche se révèle impossible ou implique des efforts disproportionnés[80]. Si c'est une impossibilité matérielle à laquelle avait pensé le législateur initialement (on ne dispose pas de données de contact relatives aux personnes concernées), une impossibilité juridique peut aussi être soulevée (l'information emporterait violation du secret professionnel)[81].

Il n'y a pas non plus d'obligation d'information lorsque l'enregistrement ou la communication des données est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance[82]. Il faut que la norme en question prévoie expressément l'enregistrement ou la communication des données[83].

B. Obligations de confidentialité et de sécurité

Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité n'aient accès et ne puissent utiliser que les données dont elles ont besoin pour

[80] Article 9, § 2, alinéa 2, a), de la loi du 8 décembre 1992.

[81] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *op. cit.*, p. 171.

[82] Article 9, § 2, alinéa 2, littera b, de la loi du 8 décembre 1992.

[83] Article 11, § 2, de la directive 95/46.

exercer leurs fonctions[84]. Il n'est pas question de permettre aux membres du personnel d'avoir accès à des données qui ne leur sont pas nécessaires.

En outre, en présence de données sensibles, le responsable doit veiller à ce que les personnes ayant accès à de telles données soient tenues par une obligation légale ou contractuelle de confidentialité[85].

Le responsable doit, en outre, mettre son personnel au courant des prescrits de la loi sur la protection des données[86]. Il doit expliquer les principes de protection qui doivent désormais être respectés.

Le responsable du traitement (auquel le RGPD ajoute le sous-traitant) doit protéger les informations qu'il a rassemblées contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Il doit prendre des mesures pour se prémunir contre la perte accidentelle de données, contre la destruction, la modification, l'accès ou tout autre traitement de données accidentel ou non autorisé[87]. Ces mesures sont l'expression de la « politique de sécurité » de l'entreprise responsable du traitement de données[88].

Ces mesures de sécurité sont de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures techniques (programme antivirus très fréquemment mis à jour, *firewalls, backup* de sécurité, *login*...).

Elles doivent assurer un niveau de protection adéquat, compte tenu de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels. Ainsi, plus les données en cause sont sensibles et les risques pour la personne concernée sont grands, plus importantes seront les précautions à prendre. Par exemple, des données relatives à la santé d'une personne, utilisées en dehors d'un contexte médical (par une compagnie d'assurances pour octroyer une assurance-vie), devront être encadrées de mesures de sécurité sévères.

On notera enfin que le RGPD généralise à l'ensemble des traitements de données l'obligation d'information en cas de « violation des données » (*data breach*), obligation qui était jusqu'ici limitée au domaine des communications électroniques[89].

Il se peut, et c'est vrai dans de nombreux cas, que l'on recoure aux services d'informaticiens ou à un service spécialisé dans le traitement des données, pour gérer les aspects

[84] Article 16, § 2, 2°, de la loi du 8 décembre 1992.

[85] Article 25, 3°, de l'arrêté royal.

[86] Article 16, § 2, 3°, de la loi du 8 décembre 1992.

[87] Article 16, § 4, de la loi.

[88] Voy. le modèle de politique de sécurité proposé par la Commission de la protection de la vie privée : *mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* disponible sur le site de la Commission, www.privacycommission.be/fr/lexique/mesures-de-reference.

[89] Voy. K. ROSIER, « Vie privée et traitement de données dans le cadre des communications électroniques », *in Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2014.

techniques des traitements de données (mise en place, alimentation et maintenance de bases de données; création et hébergement d'un site Internet, services du *Cloud* par exemple). Si les personnes auxquelles on fait appel ne sont pas sous l'autorité directe du responsable du traitement de données, elles seront considérées comme sous-traitants aux yeux de la loi de 1992[90]. Ce sera le cas notamment des sociétés extérieures, mais également de personnes ou d'un département interne à l'entreprise, mais ne se trouvant pas sous l'autorité du responsable, celui-ci étant, par exemple, un département et non la société.

Le responsable du traitement peut donc confier tout ou partie du traitement de données à caractère personnel à un sous-traitant. Il ne peut toutefois choisir celui-ci à la légère : la loi ne l'autorise à contracter qu'avec un sous-traitant qui offre des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements de données.

Par ailleurs, il s'impose aussi de baliser les relations entre responsable du traitement et sous-traitant. Le responsable doit conclure un contrat avec le sous-traitant choisi. Dans ce contrat, le sous-traitant doit obligatoirement s'engager à n'agir que sur instruction du responsable du traitement et à respecter les mesures de protection prises. Le contrat doit également fixer la responsabilité du sous-traitant vis-à-vis du responsable du traitement[91]. Le tout doit être « consigné par écrit ou sur un support électronique »[92].

VII. Transferts de données vers l'étranger[93]

A. Transfert de données personnelles vers un État membre de l'Union européenne

Les transferts de données personnelles entre pays membres de l'Union européenne sont libres. Une personne établie en Belgique peut donc librement envoyer des données personnelles dans un autre pays de l'Union européenne si cet envoi est légitime aux yeux de la loi belge (si cet envoi s'impose pour réaliser le but annoncé du traitement des données ou s'il est compatible avec ce but). Par exemple, une banque peut sans états d'âme envoyer les données relatives à un de ses clients pour effectuer un paiement en France.

B. Transfert de données personnelles hors de l'Union européenne

En dehors de l'Union européenne, on ne peut transférer des données personnelles que vers des pays qui assurent une protection des données correspondant à celle assurée sur

[90] Article 1er, § 5, de la loi du 8 décembre 1992.

[91] Article 16, § 1er, de la loi du 8 décembre 1992.

[92] Article 16, § 1er, 5°, de la loi du 8 décembre 1992.

[93] Pour une analyse détaillée, voy. C. GAYREL, « Le régime des transferts internationaux de données à caractère personnel », *in Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2014.

le territoire de l'Union européenne[94]. En l'absence d'une telle règle, la forte protection garantie à l'intérieur de l'Union européenne serait rapidement vide de sens, étant donné la facilité de circulation des données grâce aux nouvelles technologies.

Tout responsable de traitement qui souhaite exporter des données personnelles hors de l'Union européenne doit d'abord se demander si le pays destinataire assure un *niveau de protection adéquat* pour de telles données. Il faut retrouver les mêmes principes de protection que ceux établis sur le territoire européen. Pour évaluer la qualité de la protection offerte, il faut tenir compte de la législation du pays en question, des règles déontologiques appliquées, etc.[95].

Dans certains cas, on peut tout de même transférer des données vers des pays qui n'offrent *pas un niveau de protection adéquat*. C'est notamment le cas si le responsable du traitement offre lui-même, par la voie contractuelle, une protection appropriée. La protection peut ainsi être assurée au moyen d'un contrat liant celui qui envoie les données et celui qui les reçoit et contenant des garanties suffisantes au regard de la protection des données. Un modèle de clauses contractuelles types offrant des garanties suffisantes est proposé par la Commission européenne[96]. Des « règles d'entreprise contraignantes » peuvent aussi être adoptées au sein d'une multinationale.

Enfin, en l'absence de protection contractuelle ou par la voie des règles d'entreprise contraignantes, les données peuvent être transférées si les personnes concernées ont donné leur consentement indubitable au transfert de leurs données vers un tel pays, ou lorsque le transfert est nécessaire pour exécuter un contrat avec la personne concernée, ou lorsque les données proviennent d'un registre public destiné à l'information du public (par exemple, registre du commerce)[97].

[94] Article 21 de la loi du 8 décembre 1992.

[95] Une liste des pays reconnus par l'Union européenne comme offrant un niveau de protection adéquat est disponible sur le site de l'Unité « Protection des données » de la DG Justice, Droits fondamentaux et Citoyenneté de la Commission européenne à l'adresse http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[96] Il est disponible sur le site Internet de la Commission mentionné ci-avant.

[97] Article 22 de la loi du 8 décembre 1992.